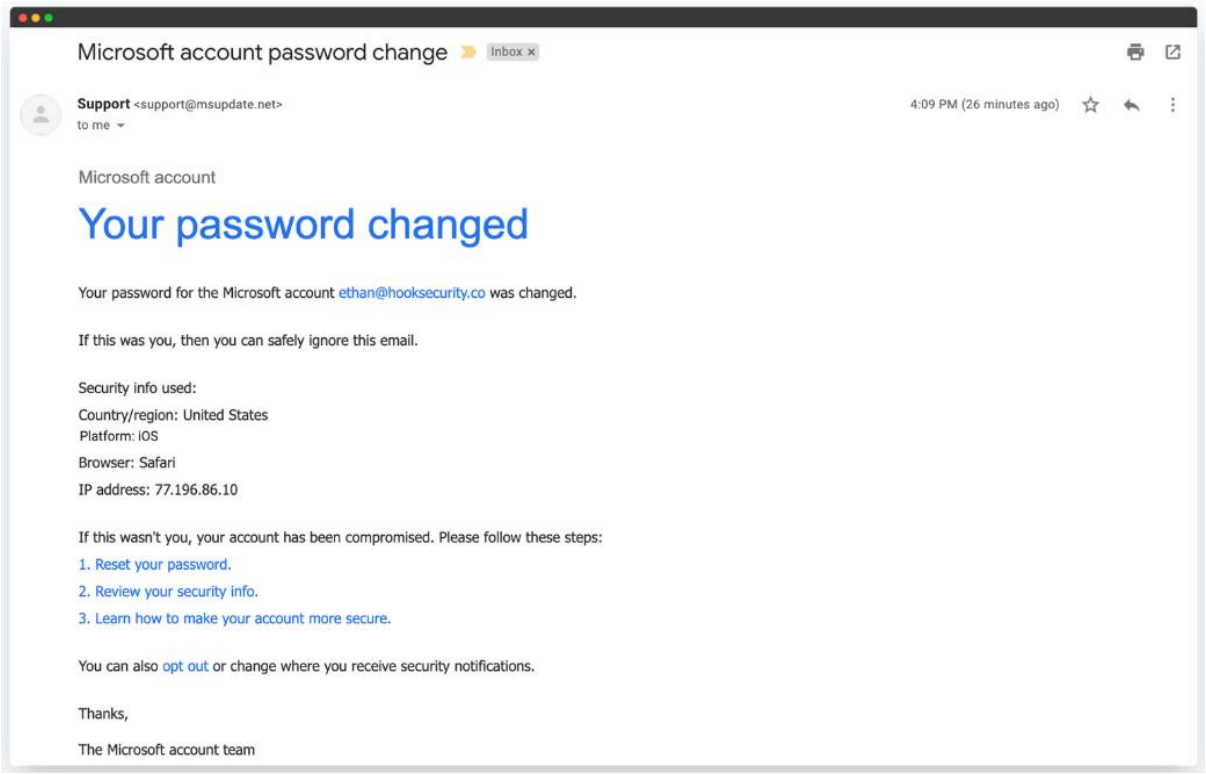
Task-2

📄 Phishing Email Analysis Report

Objective:
Identify phishing characteristics in the suspicious email sample.

🔹 1. Sender's Email Address

- **Observed:** support@msupdate.net
- 

- **Analysis:** Microsoft official emails usually come from @microsoft.com, not @msupdate.net. This is a **spoofed sender address** — very suspicious.

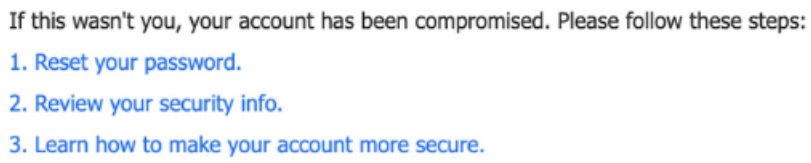
🔹 2. Email Header Analysis

- Headers not provided directly, but based on visible content:
    - The domain msupdate.net is unrelated to Microsoft → highly suspicious.

- Legitimate Microsoft security emails always use official domains.

🔹 3. Suspicious Links

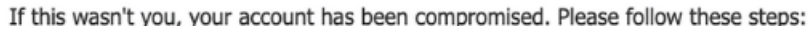
- Email contains multiple links:
  - Reset your password
  - Review your security info
  - Learn how to make your account more secure



- Links in phishing emails often redirect to fake login pages to steal credentials.
- **Recommendation:** Hover links in a safe environment (e.g., sandbox or isolated VM) to check if they point to non-Microsoft domains.

🔹 4. Urgent or Threatening Language

- Email says:
  - "If this wasn't you, your account has been compromised…"



  - Directly creates fear → classic phishing tactic.

🔹 5. Mismatched URLs

- While email text shows links pointing to supposed Microsoft actions, actual URLs behind them (not visible in screenshot) could lead to malicious websites.
- Real emails from Microsoft have verified *.microsoft.com URLs.

🔹 6. Spelling & Grammar Errors

- This email appears mostly grammatically correct → but this alone doesn't confirm legitimacy, since many phishing emails can have perfect grammar to appear more convincing.

🔷 7. Additional Observations

- The message tries to prompt **immediate action** — another sign of phishing.
- The sender uses a domain (msupdate.net) trying to look like Microsoft by including "ms" but isn't legitimate.

- Real Microsoft security emails typically include personalized details like your name and partially masked account info; here it's missing.

🔷 8. Summary of Phishing Traits

- **Spoofed sender domain**: msupdate.net is not owned by Microsoft.
- **Urgent language**: Creates fear to force quick action.
- **Suspicious links**: Links likely redirect to phishing sites.
- **Generic salutation**: Email doesn't use recipient's name → typical phishing sign.

📝 **Prepared By:** Bollineni Akshaya
📅 **Date:** 05-08-2025